



PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 13 November 2000 (13.11.00)	
International application No. PCT/EP00/02414	Applicant's or agent's file reference S 4429 WO
International filing date (day/month/year) 17 March 2000 (17.03.00)	Priority date (day/month/year) 18 March 1999 (18.03.99)
Applicant NEIFER, Wolfgang	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
 16 October 2000 (16.10.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Manu Berrod Telephone No.: (41-22) 338.83.38
--	--

This Page Blank (uspto)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 11 SEP 2001

WIPO

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

T4

Aktenzeichen des Anmelders oder Anwalts S 4429 WO	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP00/02414	Internationales Anmeldedatum (Tag/Monat/Jahr) 17/03/2000	Prioritätsdatum (Tag/Monat/Jahr) 18/03/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F1/00		
Anmelder SCM MICROSYSTEMS GMBH et al.		



RECEIVED
FEB 11 2002
Technology Center 2100

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.
☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 9 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 16/10/2000	Datum der Fertigstellung dieses Berichts 07.09.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Harms, C Tel. Nr. +49 89 2399 7476 

This Page Blank (uspto)

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

2,4,5 ursprüngliche Fassung

1,1a,3,3a eingegangen am 23/01/2001 mit Schreiben vom 23/01/2001

Patentansprüche, Nr.:

1-21 eingegangen am 23/01/2001 mit Schreiben vom 23/01/2001

Zeichnungen, Blätter:

2-4 ursprüngliche Fassung

1 eingegangen am 23/01/2001 mit Schreiben vom 23/01/2001

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

This Page Blank (uspto)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP00/02414

- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-21
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-21
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-21
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

This Page Blank (uspto)

PUNKT V

Die Erfindung beschreibt ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung und ein Wiedergabesystem zur Durchführung des Verfahrens.

Nächster Stand der Technik: D1 = DE 29802270

In D1 Seite 6 letzter Absatz ist zwar auch wie in der vorliegenden Anmeldung das SAM-Modul (Subscriber Access Modul) beschrieben, allerdings wird dort kein Verfahren zur Sicherung der Daten gegen unauthorisierte Vervielfältigung angeführt.

Durch die spezielle Abfolge und Ausführung der einzelnen Schritte hebt sich der Verfahrensanspruch 1 auch hinreichend von gängigen Übertragungsmethoden wie PGP (Pretty Good Privacy) ab, die Verschlüsselung zur sicheren Datenübertragung verwenden.

Aufgrund der im Recherchenbericht zitierten Dokumente ist der Fachmann außerstande, in offensichtlicher Weise ein Verfahren nach Hauptanspruch 1 zu entwickeln. Hauptanspruch 18 beschreibt den zu dem Methodenanspruch 1 korrespondierenden Apparat.

Somit erfüllen die Hauptansprüche die Erfordernisse von Artikel 33(2) und (3) PCT. Die Ansprüche 2-17 und 19-21 sind von den Hauptansprüchen 1 bzw. 18 abhängig und erfüllen somit ebenfalls die Erfordernisse von Artikel 33(2) und (3) PCT.

This Page Blank (uspto)

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

5 PCT/EP00/02414
 SCM Microsystems GmbH

10 Unser Zeichen: S 4429 WO
 HD

15

 Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher
 gegen unautorisierte Vervielfältigung

20 Die Erfindung betrifft ein Verfahren zur Sicherung von Daten in einem
 tragbaren Massenspeicher gegen unautorisierte Vervielfältigung und ein
 Wiedergabesystem zur Durchführung des Verfahrens.

25 Die kommerzielle Verbreitung von multimedialen Inhalten und Software
 geschieht ganz überwiegend auf Datenträgern, die nur einmal beschreib-
 bar sind und mit dem darauf gespeicherten Inhalt das Handelsprodukt
 bilden. Die kommerzielle Verbreitung der Inhalte losgelöst von solchen
30 Datenträgern wäre prinzipiell möglich, beispielsweise durch Fernzu-
 griff auf Netzwerke mit Bezahlungsfunktion, scheitert jedoch am mangelnden
 Schutz gegen unautorisierte Vervielfältigung.

35 Aus der Gebrauchsmuster-Schrift DE 298 02 270 U1 ist ein multimediales
 System mit einer Basisstation, einer tragbaren Bedieneinrichtung und
 einem Kommunikationsmodul zur Verwendung in dem multimedialen System
 bekannt. Dort wird die Kommunikation zwischen den besagten Komponenten
 bzw. zwischen dem Anwender und dem multimedialen System beschrieben,
 und es werden Möglichkeiten der Datensicherheit, wie zum Beispiel eine
40 auf einer Chipkarte implementierte Zugriffskontrolle auf eine Bestell-
 und Bezahlungsfunktion, genannt, ohne jedoch dabei explizit ein Verfahren
 zur Sicherung von Daten zu offenbaren.

This Page Blank (uspto)

- 1a -

Durch die Erfindung wird ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung zur Verfügung gestellt, das mit geringem Aufwand und verfügbarer Technologie durchgeführt werden kann. Nach dem erfindungsgemäßen Verfahren werden die Daten in dem Massenspeicher zunächst in verzerrter Form gespeichert. In einem Wiedergabesystem für die Daten wird wenigstens ein SAM-Modul (Safe Access Modul, d.h. Modul für gesicherten Zugriff) verwendet, auf dem ein persönlicher Identitätscode eines autorisierten Benutzers gespeichert ist. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf dem SAM-Modul des autorisierten Benutzers gespeichert. Den Daten wird ein Autorisierungscode zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul wird sodann ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet. Dieser verschlüsselte Autorisierungscode wird mit den verzerrten Daten auf dem Massenspeicher abgelegt. Vor einer Wiedergabe der Daten wird der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscode vom SAM-Modul entschlüsselt. Der entschlüsselte Autorisierungscode wird dann mit dem auf dem SAM-Modul (unverschlüsselt) abgelegten Autorisierungscode verglichen. Die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels der Entzerrungsschlüssel wird dann nur bei übereinstimmenden

This page blank (uspto)

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus der folgenden Beschreibung und aus der Zeichnung, auf die Bezug genommen wird. In der Zeichnung zeigen:

5 Figur 1 ein Blockschaltbild eines Wiedergabesystems zur Durchführung des erfindungsgemäßen Verfahrens;

10 Figur 2 einen Algorithmus zur Personalisierung der Daten im Massenspeicher nach dem erfindungsgemäßen Verfahren;

15 Figur 3 einen Algorithmus zur Überprüfung der Wiedergabe-Autorisierung nach dem erfindungsgemäßen Verfahren;

20 Figur 4 den Wiedergabeprozess nach dem erfindungsgemäßen Verfahren.

Das in Figur 1 gezeigte Blockschaltbild eines Wiedergabesystems zur Durchführung des erfindungsgemäßen Verfahrens zeigt schematisch die wesentlichen Komponenten des Systems. Eine in einem kompakten Gehäuse untergebrachte Schnittstelleneinrichtung ist allgemein mit 10 bezeichnet und weist drei Schnittstellen 12, 14, 16 für steckbare Komponenten sowie einen Ausgangsanschluß 18 für ein Video-Ausgabegerät 20 auf. Die Schnittstelle 12 hat einen Stecksockel für einen Massenspeicher 22, der auf einer dem Benutzer zugänglichen Fläche einen Fingerabdruck-Sensor 24 aufweist. Ein erstes SAM-Modul 26 ist Bestandteil der Schnittstelle 12. Ein zweites SAM-Modul ist in dem steckbaren Massenspeicher 22 enthalten. Dieser Massenspeicher kann eine miniaturisierte Festplatte oder auch ein Halbleiterspeicher sein, beispielsweise in FLASH-Technologie.

Die Schnittstelle 14 nimmt einen Chipkartenleser 28 im Format einer PC-Karte (Abkürzung für PCMCIA-Karte) auf. Der Chipkartenleser 28 bildet in Verbindung mit einer Chipkarte 30, auch als Smart Card bezeichnet, ein Bezahlssystem für den bedingten Zugang zu einem Anbieter multimedialer Inhalte und dergleichen, insbesondere über das Internet.

An der Schnittstelle 16 wird ein Modem 32 oder ein Netzwerkadapter angeschlossen. Über das Modem 32 oder den Netzwerkadapter kann der Zugriff auf ein entferntes Netzwerk, insbesondere das Internet, erfolgen.

This Page Blank (uspto)

- 3a -

Am Ausgangsanschluß 18, der als SCART-Schnittstelle ausgeführt sein kann, wird ein Fernsehempfänger oder Monitor angeschlossen.

5 Das Wiedergabesystem kann ferner mit einer Infrarot-Fernbedienung 34 ausgestattet sein.

This Page Blank (uspto)

Patentansprüche

1. Verfahren zur Sicherung von Daten in einem tragbaren Massen-speicher (22) gegen unautorisierte Vervielfältigung, insbesondere zum Schutz von multimedialen Informationen und Software, dadurch gekennzeichnet, daß:
- 5
- a) die Daten in dem Massenspeicher (22) in verzerrter Form gespeichert werden;
- 10
- b) in einem Wiedergabesystem für die Daten wenigstens ein persönliches Modul für gesicherten Zugriff (27), nachfolgend als SAM-Modul bezeichnet, verwendet wird, auf dem ein persönlicher Identitätscode des autorisierten Benutzers gespeichert ist;
- 15
- c) wenigstens ein zur Entzerrung der Daten benötigter Entzerrungsschlüssel auf dem SAM-Modul (27) des autorisierten Benutzers gespeichert wird;
- 20
- d) den Daten ein Autorisierungs-Code zugeordnet wird, der auf dem SAM-Modul (27) abgelegt wird;
- e) auf dem SAM-Modul (27) ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet wird;
- 25
- f) der verschlüsselte Autorisierungscode auf dem Massenspeicher (22) abgelegt wird;
- g) vor einer Wiedergabe der Daten der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul (27) entschlüsselt wird;
- 30
- h) der entschlüsselte Autorisierungscode mit dem auf dem SAM-Modul (27) abgelegten Autorisierungscode verglichen wird und die Entzerrung der vom Massenspeicher (22) ausgelesenen Daten mittels des Entzerrungsschlüssels nur bei übereinstimmenden Autorisierungscodes freigegeben wird.
- 35

This Page Blank (uspto)

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vor dem Erwerb der Daten von einem Anbieter ein System-Zertifikat vom SAM-Modul zum Anbieter gesendet und von diesem überprüft wird.
- 5 3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für die gesicherte Übertragung des Autorisierungscode zum SAM-Modul des autorisierten Benutzers ein Sitzungsschlüssel verwendet wird.
- 10 4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zur Personalisierung der Daten auf dem Massenspeicher (22) eine Kennzeichnung aus persönlichen Merkmalen des autorisierten Benutzers gebildet und mit den Daten in solcher Weise verknüpft wird, daß die Daten nur mit der Kennzeichnung ausgegeben werden können.
- 15 5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der persönliche Identitätscode des autorisierten Benutzers zumindest teilweise aus von einem Fingerabdruck-Sensor (24) gelieferten Daten gebildet wird.
- 20 6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher (22) in einem an einem Wiedergabesystem steckbaren Modul angeordnet ist.
- 25 7. Verfahren nach den Ansprüchen 5 und 6, dadurch gekennzeichnet, daß der Fingerabdruck-Sensor (24) auf einer Fläche des steckbaren Moduls angeordnet ist.
- 30 8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß mittels eines ersten, im Wiedergabesystem angeordneten SAM-Moduls (26) die Kommunikation und Transaktion mit dem Anbieter der Daten und mittels eines zweiten, dem Massenspeicher (22) zugeordneten SAM-Moduls (27) die Personalisierung der Daten abgewickelt werden.
- 35 9. Verfahren nach den Ansprüchen 6 und 8, dadurch gekennzeichnet, daß das dem Massenspeicher (22) zugeordnete SAM-Modul (27) in das steckbare Modul integriert ist.
- 40 10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher (22) als miniaturisierte Festplatte ausgebildet ist.

This Page Blank (uspto)

11. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Massenspeicher (22) als Flash-Halbleiterspeicher ausgebildet ist.
- 5 12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß der Flash-Halbleiterspeicher entfernbar in einem am Wiedergabesystem steckbaren Schnittstellen-Modul angeordnet ist.
- 10 13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß das Schnittstellen-Modul einen SAM-Kartenleser enthält.
14. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zum Erwerb der Daten eine Kommunikation und Transaktion mit einem Anbieter per Fernzugriff auf ein Netzwerk erfolgt.
- 15 15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß die Transaktion mit dem Anbieter unter Verwendung eines in das Wiedergabesystem einsteckbaren Kartenleser-Moduls erfolgt, das einen Chipkartenleser (28) und einen das wenigstens eine SAM-Modul (26) aufnehmenden SAM-Kartenleser beinhaltet.
- 20 16. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Entzerrungsschlüssel seinerseits mit auf dem SAM-Modul gespeicherten persönlichen Daten chiffriert und bei der Wiedergabe mit diesen Daten dechiffriert wird.
- 25 17. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß ein zertifizierter Zeitstempel erzeugt und mit den Daten auf dem Massenspeicher (22) gespeichert wird.
- 30 18. Wiedergabesystem zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, gekennzeichnet durch:
- ein Lesemodul zur Aufnahme des Massenspeichers (22);
 - 35 - einen Kartenleser (28) für das SAM-Modul;
 - eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher (22) gelesenen Daten; und
 - ein Ausgabegerät (20) für die entzerrten Daten.
- 40 19. Wiedergabesystem nach Anspruch 16, ferner gekennzeichnet durch ein auf einem Chipkartenleser (28) basierendes Bezahlssystem für bedingten Zugang zu einem Datenanbieter über ein entferntes Netzwerk.

This Page Blank (uspto)

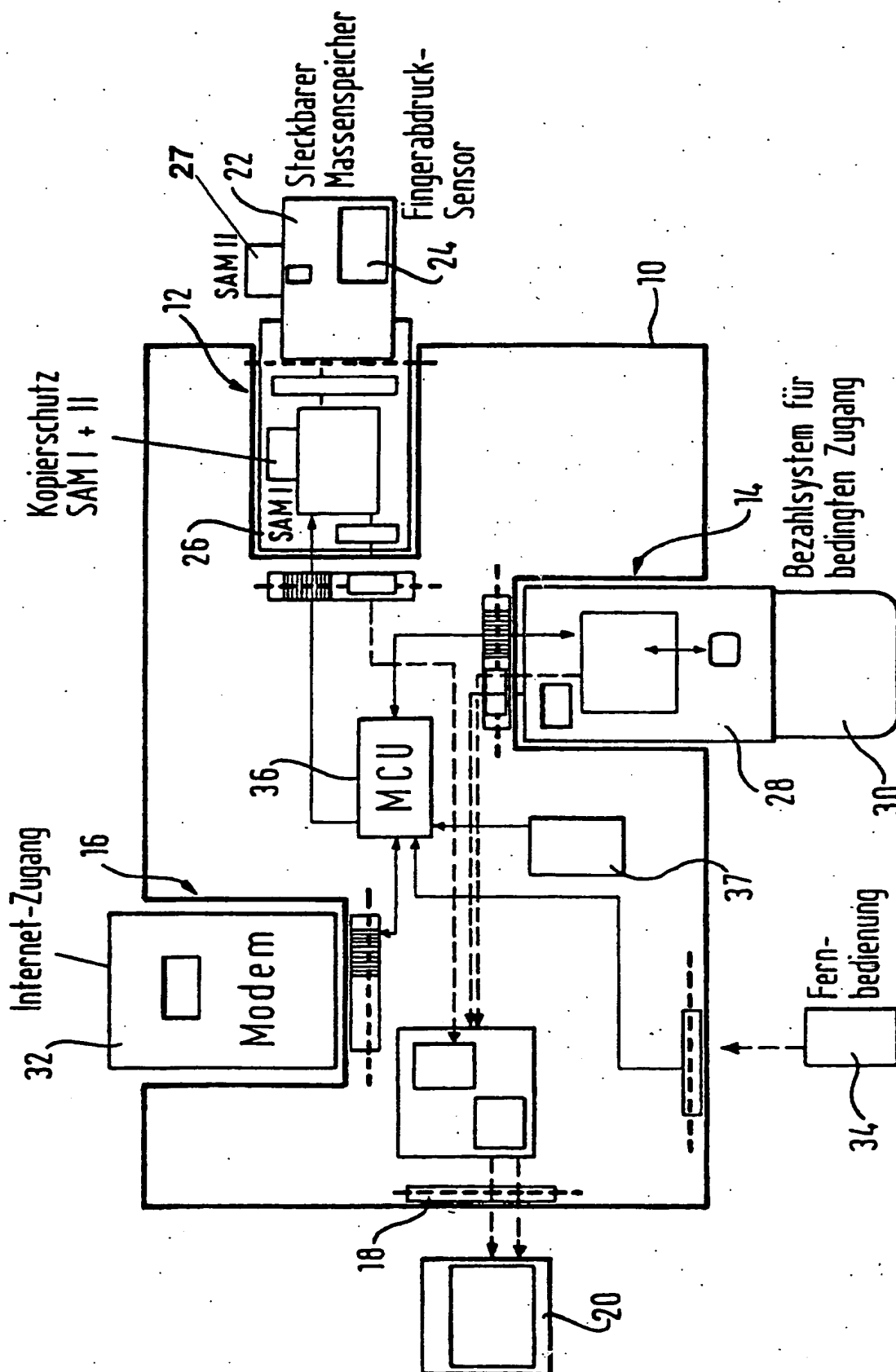
20. Wiedergabesystem nach Anspruch 17, dadurch gekennzeichnet, daß der Chipkartenleser (28) als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

- 5 21. Wiedergabesystem nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß eine Überwachungseinrichtung vorgesehen ist, die einen mit den Daten vom Massenspeicher (22) gelesenen zertifizierten Zeitstempel auswertet.

10

This Page Blank (uspto)

Fig. 1



This Page Blank (uspto)

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference S 4429 WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP00/02414	International filing date (day/month/year) 17 March 2000 (17.03.00)	Priority date (day/month/year) 18 March 1999 (18.03.99)
International Patent Classification (IPC) or national classification and IPC G06F 1/00, G11B 20/00		RECEIVED NOV 16 2001 Technology Center 2100
Applicant SCM MICROSYSTEMS GMBH		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 4 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 9 sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 16 October 2000 (16.10.00)	Date of completion of this report 07 September 2001 (07.09.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

this Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP00/02414

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments):*

- ☒ the international application as originally filed.
- ☒ the description, pages 2,4,5, as originally filed,
pages _____, filed with the demand,
pages 1,1a,3,3a, filed with the letter of 23 January 2001 (23.01.2001),
pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-21, filed with the letter of 23 January 2001 (23.01.2001),
Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 2-4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig 1, filed with the letter of 23 January 2001 (23.01.2001),
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP 00/02414

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-21	YES
	Claims		NO
Inventive step (IS)	Claims	1-21	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-21	YES
	Claims		NO

2. Citations and explanations

The invention describes a method for securing data in a portable mass memory against unauthorised reproduction and a playback system for carrying out the method.

Closest prior art: DE-A-298 02 270 (D1).

The final paragraph of page 6 of D1 describes the SAM module, as in the present application, but does not indicate a method for securing data against unauthorised reproduction.

The special sequence and execution of the individual steps distinguish method Claim 1 sufficiently from standard transfer methods such as PGP (Pretty Good Privacy), which use encryption to ensure secure data transfer.

The search report citations do not enable a person skilled in the art to develop a method according to the main Claim 1 in an obvious manner. The main Claim 18 describes the apparatus corresponding to method Claim 1.

Consequently, the main claims meet the requirements of PCT Article 33(2) and (3). Claims 2-17 and 19-21 are dependent on the main Claims 1 and 18 and therefore likewise meet

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 00/02414

the requirements of PCT Article 33(2) and (3).

This Page Blank (uspto)

**REPLACED BY
ANT 34 AMST**

PCT/EP00/02414
SCM Microsystems GmbH

Our file: S 4429 WO
HD/me

5 A Method of Securing Data in a Portable Mass Storage against Unauthorized Copying

The invention relates to a method of securing data in a portable mass storage against unauthorized copying and a replay system for performing the method.

- 10 Multimedia contents and software are quite predominantly disseminated commercially on data carriers which can be written to only once and constitute the trade product together with the contents stored thereon. A separate commercial dissemination of the contents independent of such data carriers would in principle be possible, for instance by remote access to networks including a payment function, but fails because
- 15 of a lack of protection against unauthorized copying.

- From Utility Model Document DE 298 02 270 U1 there is known a multimedia system comprising a base station, a portable operating device and a communication module for use in the multimedia system. In this reference, the communication between the aforesaid components and between the user and the multimedia system, respectively,
- 20 is described; there are also quoted possibilities for the data security such as a supervision, implemented on a chip card, of an access to an order and payment function, without, however, explicitly disclosing a method of securing data.

AMENDED SHEET

1005 8 1 1978

2005 8 1 1978

This Page Blank (uspto)

The invention provides a method of securing data in a portable mass storage against unauthorized copying, which can be performed with little expenditure and using available technology. In accordance with the method of the invention the data is first stored in the mass storage in a scrambled form. In a replay system for the data at least
5 one SAM module (Safe Access Module) is used which has stored thereon a personal identity code of an authorized user. The descrambling keys required for descrambling the data are stored on the SAM module of the authorized user. Assigned to the data is an authorization code which is stored on the SAM module. Then an authorization code encoded by means of the personal identity code is formed on the SAM module. This
10 encoded authorization code is stored on the mass storage with the scrambled data. Prior to a replay of the data, the encoded authorization code is decoded by the SAM module by means of the personal identity code. The decoded authorization code is then compared with the authorization code stored (non-encoded) on the SAM module. The descrambling by means of the descrambling keys of the data read out of the mass
15 storage is then enabled only when [the authorization codes are identical.]

This Page Blank (uspto)

Further advantages and features of the present invention will be apparent from the following description and from the drawings to which reference is made and in which:

Fig. 1 is a block diagram of a replay system for carrying out the method according to the invention;

5 Fig. 2 shows an algorithm for the personalization of the data in the mass storage according to the method of the invention;

Fig. 3 shows an algorithm for checking the replay authorization according to the method of the invention;

Fig. 4 shows the replay process according to the method of the invention.

10 The block diagram as shown in Figure 1 of a replay system for performing the method in accordance with the invention diagrammatically shows the essential components of the system. An interface device accommodated in a compact housing is generally denoted by reference number 10 and comprises three interfaces 12, 14, 16 for plug-in type components as well as an output terminal 18 for a video output device 20.

15 The interface 12 has a plug-in socket for a mass storage 22 which has a fingerprint sensor 24 on a surface accessible to the user. A first SAM module 26 is a part of the interface 12. A second SAM module is contained in the plug-in type mass storage 22, which may be a miniaturized hard disk or also a semiconductor storage, for instance in FLASH technology.

20 The interface 14 accommodates a chip card reader 28 in the format of a PC card (abbreviation for PCMCIA card). In conjunction with a chip card 30, also referred to as smart card, the chip card reader 28 constitutes a payment system for the conditional access to a provider of multimedia contents and the like, in particular via the Internet.

25 Connected to the interface 16 is a modem 32 or a network adapter. Via the modem 32 or the network adapter a remote network may be accessed, more particularly the Internet.

This Page Blank (uspto)

- 3a -

A television set or a monitor is connected to the output terminal 18, which may be designed as a SCART interface.

The replay system may further be fitted with an infrared remote control 34.

AMENDED SHEET

This Page Blank (uspto)

Claims

1. A method of securing data in a portable mass storage (22) against unauthorized copying, in particular for the protection of multimedia information and software, characterized in that:
- 5 a) the data is stored in the mass storage (22) in a scrambled form;
- b) in a replay system for the data at least one personal SAM module for secured access (27), in the following referred to as SAM module, is used which has stored thereon a personal identity code of the authorized user;
- 10 c) at least one descrambling key required for descrambling the data is stored on the SAM module (27) of the authorized user;
- d) an authorization code is assigned to the data and is stored on the SAM module (27);
- e) an authorization code encoded by means of the personal identity code is
- 15 formed on the SAM module (27);
- f) the encoded authorization code is stored on the mass storage (22);
- g) prior to a replay of the data, the encoded authorization code is decoded by the SAM module (27) by means of the personal identity code;
- h) the decoded authorization code is compared with the authorization code
- 20 stored on the SAM module (27), and descrambling by means of the descrambling key of the data read out of the mass storage (22) is enabled only when the authorization codes are identical.

This Page Blank (uspto)

2. The method according to claim 1; characterized in that prior to the purchase of the data from a provider, a system certificate is transmitted from the SAM module to the provider and verified by the latter.

5 3. The method according to claim 1 or 2, characterized in that a session key is used for the secured transfer of the authorization code to the SAM module of the authorized user.

4. The method according to any of the preceding claims, characterized in that for personalizing the data on the mass storage (22) an identification consisting of personal features of the authorized user is formed and linked with the data in
10 such a manner that the data can be output only with the identification.

5. The method according to any of the preceding claims, characterized in that the personal identity code of the authorized user is formed at least in part from data supplied by a fingerprint sensor (24).

6. The method according to any of the preceding claims, characterized in
15 that the mass storage (22) is arranged in a module adapted to be plugged into a replay system.

7. The method according to claims 5 and 6, characterized in that the fingerprint sensor (24) is arranged on a surface of the plug-in type module.

8. The method according to any of the preceding claims, characterized in
20 that the communication and transaction with the provider of the data is conducted by means of a first SAM module (26) arranged in the replay system, and the personalization of the data is carried out by means of a second SAM module (27) assigned to the mass storage (22).

9. The method according to claims 6 and 8, characterized in that the SAM
25 module (27) assigned to the mass storage (22) is integrated in the plug-in type module.

10. The method according to any of the preceding claims, characterized in that the mass storage (22) is configured as a miniaturized hard disk.

This Page Blank (uspto)

11. The method according to any of claims 1 to 9, characterized in that the mass storage (22) is configured as flash semiconductor storage.

12. The method according to claim 11, characterized in that the flash semiconductor storage is removably arranged in an interface module adapted to be plugged into the replay system.

13. The method according to claim 12, characterized in that the interface module comprises a SAM card reader.

14. The method according to any of the preceding claims, characterized in that for purchasing the data a communication and transaction with a provider is effected by means of a remote access to a network.

15. The method according to claim 14, characterized in that the transaction with the provider is effected using a card reader module which is adapted to be plugged into the replay system and which includes a chip card reader (28) and a SAM card reader accommodating the at least one SAM module (26).

16. The method according to any of the preceding claims, characterized in that the descrambling key is for its part encrypted with personal data stored on the SAM module and is decrypted with such data during replay.

17. The method according to any of the preceding claims, characterized in that a certified time stamp is generated and stored with the data on the mass storage (22).

18. A replay system for performing the method according to any of the preceding claims, characterized by:

- a read module for accommodating the mass storage (22);
- a card reader (28) for the SAM module;
- a data conditioning electronics for descrambling the data read out of the mass storage (22); and
- an output device (20) for the descrambled data.

19. The replay system according to claim 16, further characterized by a payment system based on a chip card reader (28), for conditional access to a data provider via a remote network.

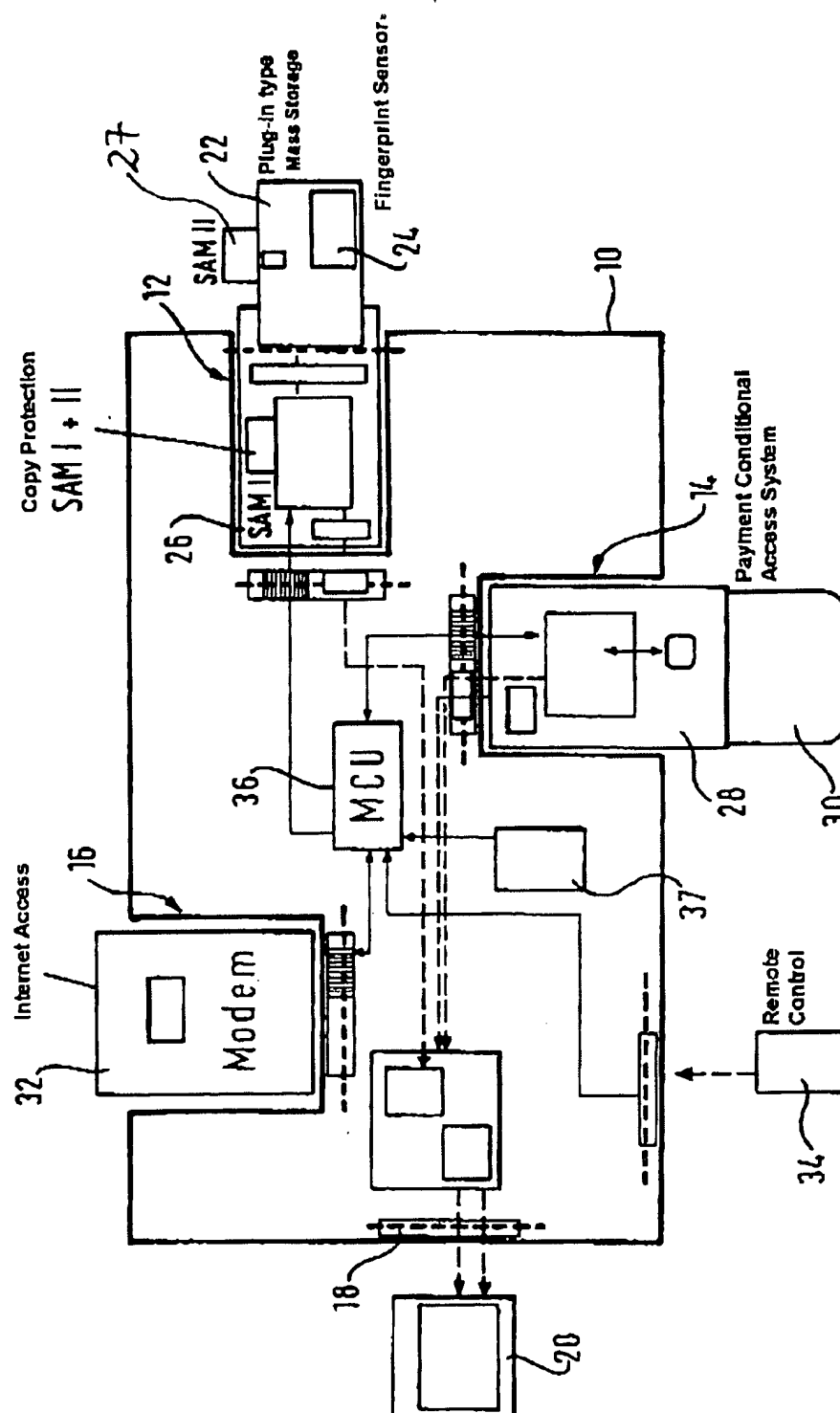
This Page Blank (uspto)

20. The replay system according to claim 17, characterized in that the chip card reader (28) is configured as a plug-in type PC card in the PCMCIA format.

5 21. The replay system according to any of claims 18 to 20, characterized in that a monitoring device is provided which evaluates a certified time stamp read out of the mass storage (22) with the data.

This Page Blank (uspto)

Fig. 1



This Page Blank (uspto)

09/936615

JC16 Rec'd PCT/PTO SEP 17 2001

TRANSLATION OF THE
Annexes (amended sheets) to the Preliminary Examination Report

2100000000

1000 1000 1000

This Page Blank (uspto)


 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

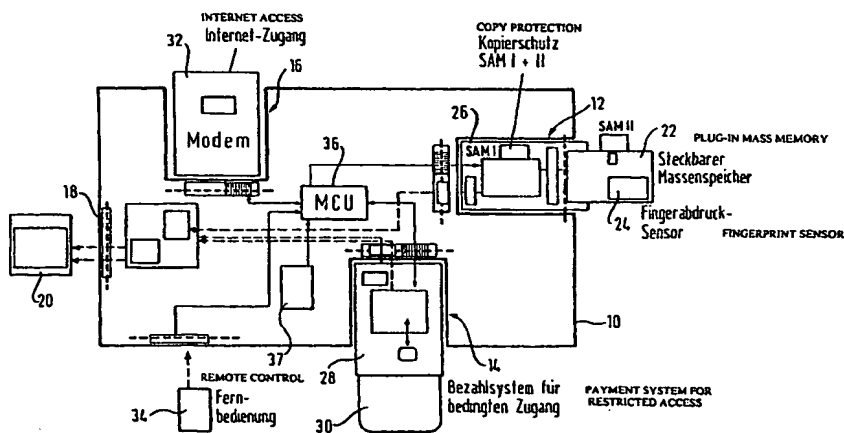
(51) Internationale Patentklassifikation ⁷ : G06F 1/00, G11B 20/00	A1	(11) Internationale Veröffentlichungsnummer: WO 00/55707 (43) Internationales Veröffentlichungsdatum: 21. September 2000 (21.09.00)
(21) Internationales Aktenzeichen: PCT/EP00/02414 (22) Internationales Anmeldedatum: 17. März 2000 (17.03.00) (30) Prioritätsdaten: 199 12 224.5 18. März 1999 (18.03.99) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenhausen, D-85276 Pfaffenhofen (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): NEIFER, Wolfgang [DE/DE]; Rosenstrasse 9a, D-85354 Freising (DE). (74) Anwalt: DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, D-81241 München (DE).		(81) Bestimmungsstaaten: JP, SG, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Mit internationalem Recherchenbericht.</i> <i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>

(54) Title: METHOD OF SECURING DATA IN A PORTABLE MASS MEMORY AGAINST UNAUTHORIZED DUPLICATION

(54) Bezeichnung: VERFAHREN ZUR SICHERUNG VON DATEN IN EINEM TRAGBAREN MASSENSPEICHER GEGEN UNAUTORISIERTE VERVIELFÄLTIGUNG

(57) Abstract

To secure multimedia information and software stored in a portable mass memory (22) against unauthorized duplication the data are stored in said mass memory (22) in distorted form. In the system (10) for playing back the data a personal identity code of the authorized user is stored in a personal serial analog memory (SAM) module. The correction keys necessary for correction of the data are stored in the SAM module of the authorized user. An authorization code is assigned to said data, which is also stored in the SAM module. An authorization code encoded by means of the personal identity code is generated in the SAM module and then stored in the mass memory (22). Before the data are played back the encoded authorization code is decoded by the SAM module by means of the personal identity code. The decoded authorization code is then compared with the authorization code stored in the SAM module and correction by means of the correction key of the data read out from the mass memory (22) is approved only if the authorization codes coincide.



(57) Zusammenfassung

Zur Sicherung von multimedialen Informationen und Software in einem tragbaren Massenspeicher (22) gegen unautorisierte Vervielfältigung werden die Daten in dem Massenspeicher (22) in verzerrter Form gespeichert. In dem Wiedergabesystem (10) für die Daten wird auf einem persönlichen SAM-Modul ein persönlicher Identitätscode des autorisierten Benutzers gespeichert. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf den SAM-Modul des autorisierten Benutzers gespeichert. Den Daten wird ein Autorisierungs-Code zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul wird ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet und dann auf dem Massenspeicher (22) abgelegt. Vor der Wiedergabe der Daten wird der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul entschlüsselt. Der entschlüsselte Autorisierungscode wird mit dem auf dem SAM-Modul abgelegten Autorisierungscode verglichen. Die Entzerrung der vom Massenspeicher (22) ausgelesenen Daten mittels des Entzerrungsschlüssels wird nur bei übereinstimmenden Autorisierungscode freigegeben.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung

5 Die Erfindung betrifft ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung und ein Wiedergabesystem zur Durchführung des Verfahrens.

10 Die kommerzielle Verbreitung von multimedialen Inhalten und Software geschieht ganz überwiegend auf Datenträgern, die nur einmal beschreibbar sind und mit dem darauf gespeicherten Inhalt das Handelsprodukt bilden. Die kommerzielle Verbreitung der Inhalte losgelöst von solchen Datenträgern wäre prinzipiell möglich, beispielsweise durch Fernzugriff auf Netzwerke mit Bezahlfunktion, 15 scheitert jedoch am mangelnden Schutz gegen unautorisierte Vervielfältigung.

20 Durch die Erfindung wird ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung zur Verfügung gestellt, das mit geringem Aufwand und verfügbarer Technologie durchgeführt werden kann. Nach dem erfindungsgemäßen Verfahren werden die Daten in dem Massenspeicher zunächst in verzerrter Form gespeichert. In einem Wiedergabesystem für die Daten wird wenigstens ein SAM-Modul (Safe Access Modul, d.h. Modul für gesicherten Zugriff) 25 verwendet, auf dem ein persönlicher Identitätscode eines autorisierten Benutzers gespeichert ist. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf dem SAM-Modul des autorisierten Benutzers gespeichert. Den Daten wird ein Autorisierungscode zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul 30 wird sodann ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet. Dieser verschlüsselte Autorisierungscode wird mit den verzerrten Daten auf dem Massenspeicher abgelegt. Vor einer Wiedergabe der Daten wird der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscode vom SAM-Modul 35 entschlüsselt. Der entschlüsselte Autorisierungscode wird dann mit dem auf dem SAM-Modul (unverschlüsselt) abgelegten Autorisierungscode verglichen. Die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels der Entzerrungsschlüssel wird dann nur bei übereinstimmenden

- 2 -

Autorisierungscode freigegeben. Durch dieses mit einfachster Hardware durchführbare Verfahren erfolgt eine Personalisierung der Daten auf dem Massenspeicher. Für die unverzerrte Wiedergabe der Daten wird ein Autorisierungscode benötigt, der nur über den SAM-Modul des autorisierten Benutzers gewonnen werden kann, weil er mit dem persönlichen Identitätscode des autorisierten Benutzers verknüpft ist.

In Weiterbildung des Verfahrens werden auch die für die Entzerrung der Daten benötigten Entzerrungsschlüssel mit auf dem SAM-Modul gespeicherten persönlichen Daten des autorisierten Benutzers chiffriert, so daß sie nur unter Verwendung des zutreffenden SAM-Moduls dechiffriert werden können.

In weiterer Ausgestaltung des Verfahrens werden die Daten bei der Wiedergabe über ein geeignetes Wiedergabesystem unlösbar mit einer persönlichen Kennzeichnung des autorisierten Benutzers ausgegeben. Die persönliche Kennzeichnung kann in einem Logo oder dergleichen bestehen, das bei Bilddaten in einer Ecke des Bildfeldes angezeigt wird.

Das erfindungsgemäße Wiedergabesystem zur Durchführung des Verfahrens enthält im wesentlichen: Ein Lesemodul zur Aufnahme des Massenspeichers, bei dem es sich vorzugsweise um ein vom Anwender beschreibbares Medium handelt, beispielsweise eine miniaturisierte Festplatte oder eine vom Benutzer beschreibbare optische Speicherplatte; einen Kartenleser für das SAM-Modul; eine Datenaufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und ein Ausgabegerät für die entzerrten Daten. Um Daten über ein entferntes Netzwerk, beispielsweise aus dem Internet, beziehen zu können, ist vorzugsweise zusätzlich ein Bezahlssystem für den bedingten Zugang zu einem Datenanbieter über das entfernte Netzwerk vorgesehen. Das Bezahlssystem basiert auf einem Chipkartenleser, der bei der bevorzugten Ausführungsform als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

35

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus der folgenden Beschreibung und aus der Zeichnung, auf die Bezug genommen wird. In der Zeichnung zeigen:

5 Das in Figur 1 gezeigte Blockschaltbild eines Wiedergabesystems zur Durchführung des erfindungsgemäßen Verfahrens zeigt schematisch die wesentlichen Komponenten des Systems. Eine in einem kompakten Gehäuse untergebrachte Schnittstelleneinrichtung ist allgemein mit 10 bezeichnet und weist drei Schnittstellen 12, 14, 16 für steckbare Komponenten sowie einen Ausgangsanschluß 18 für ein Video-Ausgabegerät 20 auf. Die Schnittstelle 12 hat einen Stecksockel für einen Massenspeicher 22, der auf einer dem Benutzer zugänglichen Fläche einen Fingerabdruck-Sensor 24 aufweist. Ein erstes SAM-Modul 26 ist Bestandteil der Schnittstelle 12. Ein zweites SAM-Modul ist in dem 15 steckbaren Massenspeicher 22 enthalten. Dieser Massenspeicher kann eine miniaturisierte Festplatte oder auch ein Halbleiterspeicher sein, beispielsweise in FLASH-Technologie.

Die Schnittstelle 14 nimmt einen Chipkartenleser 28 im Format einer PC-Karte (Abkürzung für PCMCIA-Karte) auf. Der Chipkartenleser 20 28 bildet in Verbindung mit einer Chipkarte 30, auch als Smart Card bezeichnet, ein Bezahlssystem für den bedingten Zugang zu einem Anbieter multimedialer Inhalte und dergleichen, insbesondere über das Internet.

25 An der Schnittstelle 16 wird ein Modem 32 oder ein Netzwerkadapter angeschlossen. Über das Modem 32 oder den Netzwerkadapter kann der Zugriff auf ein entferntes Netzwerk, insbesondere das Internet, erfolgen.

30 Am Ausgangsanschluß 18, der als SCART-Schnittstelle ausgeführt sein kann, wird ein Fernsehempfänger oder Monitor angeschlossen.

Das Wiedergabesystem kann ferner mit einer Infrarot-Fernbedienung 35 34 ausgestattet sein.

Ein interner Prozessor 36 beinhaltet die notwendige Funktionalität zur Entzerrung und Aufbereitung der von dem Massenspeicher 22 ausgelesenen Daten für die Wiedergabe auf dem Ausgabegerät 20. Der Prozessor 36 ist mit einem synchronisierten Zeitgeber 37 gekoppelt, der Bestandteil einer Überwachungseinrichtung ist, mittels welcher die Aufbereitung der Daten zur Wiedergabe von einem zertifizierten Zeitstempel abhängig gemacht wird, der mit den Daten auf dem Massenspeicher 22 aufgezeichnet ist.

Das erfindungsgemäße Verfahren ist in den Diagrammen der Figuren 2, 3 und 4 dargestellt. Es besteht im wesentlichen aus drei Stufen. In der ersten, in Figur 2 dargestellten Stufe des Verfahrens erfolgt eine Personalisierung der Daten im Massenspeicher. Der Vorgang wird mit der Übersendung eines System-Zertifikats zum Anbieter der Daten begonnen. Bei den Daten handelt es sich insbesondere um multimediale Informationen, abgekürzt als MMI. Durch das Systemzertifikat weist sich das Wiedergabesystem beim MMI-Anbieter als geeignetes System aus. Seitens des MMI-Anbieters wird dann aus dem SAM-Modul des Wiedergabesystems ein privater Schlüssel empfangen, um einen Wiedergabe-Autorisierungscode zu erzeugen. Bei dem privaten Schlüssel kann es sich um einen persönlichen Identitätscode oder auch um vom Fingerabdruck-Sensor 24 abgeleitete komprimierte Daten, oder eine Kombination derselben, handeln. Der Wiedergabe-Autorisierungscode wird dann auf dem SAM-Modul gespeichert.

Anschließend erfolgt mittels des Bezahlsystems 28, 30, die Bezahlung, woraufhin die MMI-Daten in verzerrter Form heruntergeladen und auf dem MMI-Massenspeicher 22 gespeichert werden. Anschließend werden die zur Entzerrung der MMI-Daten benötigten MMI-Schlüssel in chiffrierter Form zum SAM-Modul übertragen und dort gespeichert. Ferner wird vom MMI-Anbieter ein chiffriertes Wasserzeichen gesendet, das im SAM-Modul gespeichert werden kann, wenn der Umfang der entsprechenden Daten vergleichsweise gering ist; andernfalls erfolgt die Speicherung im Massenspeicher. Optional wird mit den MMI-Daten ein zertifizierter Zeitstempel gesendet und auf dem Massenspeicher 22 aufgezeichnet.

Als letzter Schritt der ersten Verfahrensstufe wird vom MMI-Anbieter ein chiffrierter Autorisierungscode gesendet, der im MMI-Massenspeicher zusammen mit den MMI-Daten gespeichert wird.

5 Wenn in den privaten Schlüssel die durch den Fingerabdruck-Sensor abgegebenen Daten eingehen, können diese durch den im Massenspeicher 22 integrierten SAM-Modul ver- oder bearbeitet werden.

10 Die in Figur 3 gezeigte Verfahrensstufe betrifft die Überprüfung der Wiedergabe-Autorisierung. In dem SAM-Modul wird dazu der aus dem Massenspeicher gelesene chiffrierte Autorisierungscode mittels des privaten Schlüssels dechiffriert; der so zurückgewonnene Autorisierungscode wird dann mit dem auf dem SAM-Modul gespeicherten Autorisierungscode verglichen. Bei übereinstimmenden Autorisierungscodes
15 wird der Wiedergabeprozess freigegeben.

Bei dem in Figur 4 gezeigten Wiedergabe-Prozess wird zunächst im SAM-Modul der MMI-Schlüssel mittels des privaten Schlüssels dechiffriert. Dann werden die MMI-Daten aus dem Massenspeicher
20 ausgelesen und mittels des dechiffrierten MMI-Schlüssels entzerrt. Die entzerrten MMI-Daten werden dann mit dem persönlichen Logo bzw. Wasserzeichen überlagert und an das Ausgabegerät abgegeben.

Durch den optional mit den MMI-Daten aufgezeichneten zertifizierten Zeitstempel kann die zugelassene Wiedergabe der Daten zeitlich befristet werden.
25

Patentansprüche

5 1. Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung, insbesondere zum Schutz von multimedialen Informationen und Software, dadurch gekennzeichnet, daß:

10 a) die Daten in dem Massenspeicher in verzerrter Form gespeichert werden;

b) in einem Wiedergabesystem für die Daten wenigstens ein persönlicher SAM-Modul verwendet wird, auf dem ein persönlicher Identitätscode des autorisierten Benutzers gespeichert ist;

15 c) wenigstens ein zur Entzerrung der Daten benötigter Entzerrungsschlüssel auf dem SAM-Modul des autorisierten Benutzers gespeichert wird;

20 d) den Daten ein Autorisierungs-Code zugeordnet wird, der auf dem SAM-Modul abgelegt wird;

e) auf dem SAM-Modul ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet wird;

25 f) der verschlüsselte Autorisierungscode auf dem Massenspeicher abgelegt wird;

30 g) vor einer Wiedergabe der Daten der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul entschlüsselt wird;

35 h) der entschlüsselte Autorisierungscode mit dem auf dem SAM-Modul abgelegten Autorisierungscode verglichen wird und die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels des Entzerrungsschlüssels nur bei übereinstimmenden Autorisierungscodes freigegeben wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vor dem Erwerb der Daten von einem Anbieter ein System-Zertifikat vom SAM-Modul zum Anbieter gesendet und von diesem überprüft wird.

5 3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für die gesicherte Übertragung des Autorisierungscode zum SAM-Modul des autorisierten Benutzers ein Sitzungsschlüssel verwendet wird.

10 4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zur Personalisierung der Daten auf dem Massenspeicher eine Kennzeichnung aus persönlichen Merkmalen des autorisierten Benutzers gebildet und mit den Daten in solcher Weise verknüpft wird, daß die Daten nur mit der Kennzeichnung ausgegeben werden können.

15 5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der persönliche Identitätscode des autorisierten Benutzers zumindest teilweise aus von einem Fingerabdruck-Sensor gelieferten Daten gebildet wird.

20 6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher in einem an einem Wiedergabesystem steckbaren Modul angeordnet ist.

25 7. Verfahren nach den Ansprüchen 5 und 6, dadurch gekennzeichnet, daß der Fingerabdruck-Sensor auf einer Fläche des steckbaren Moduls angeordnet ist.

30 8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß mittels eines ersten, im Wiedergabesystem angeordneten SAM-Moduls die Kommunikation und Transaktion mit dem Anbieter der Daten und mittels eines zweiten, dem Massenspeicher zugeordneten SAM-Moduls die Personalisierung der Daten abgewickelt werden.

35 9. Verfahren nach den Ansprüchen 6 und 8, dadurch gekennzeichnet, daß das dem Massenspeicher zugeordnete SAM-Modul in das steckbare Modul integriert ist.

10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher als miniaturisierte Festplatte ausgebildet ist.

5 11. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Massenspeicher als Flash-Halbleiterspeicher ausgebildet ist.

10 12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß der Flash-Halbleiterspeicher entfernbar in einem am Wiedergabesystem steckbaren Schnittstellen-Modul angeordnet ist.

15 13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß das Schnittstellen-Modul einen SAM-Kartenleser enthält.

20 14. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zum Erwerb der Daten eine Kommunikation und Transaktion mit einem Anbieter per Fernzugriff auf ein Netzwerk erfolgt.

25 15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß die Transaktion mit dem Anbieter unter Verwendung eines in das Wiedergabesystem einsteckbaren Kartenleser-Moduls erfolgt, das einen Chipkartenleser und einen das wenigstens eine SAM-Modul aufnehmenden SAM-Kartenleser beinhaltet.

30 16. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Entzerrungsschlüssel seinerseits mit auf dem SAM-Modul gespeicherten persönlichen Daten chiffriert und bei der Wiedergabe mit diesen Daten dechiffriert wird.

35 17. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß ein zertifizierter Zeitstempel erzeugt und mit den Daten auf dem Massenspeicher gespeichert wird.

18. Wiedergabesystem zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, gekennzeichnet durch:

- 5 - ein Lesemodul zur Aufnahme des Massenspeichers;
- einen Kartenleser für das SAM-Modul;
- eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und
- ein Ausgabegerät für die entzerrten Daten.

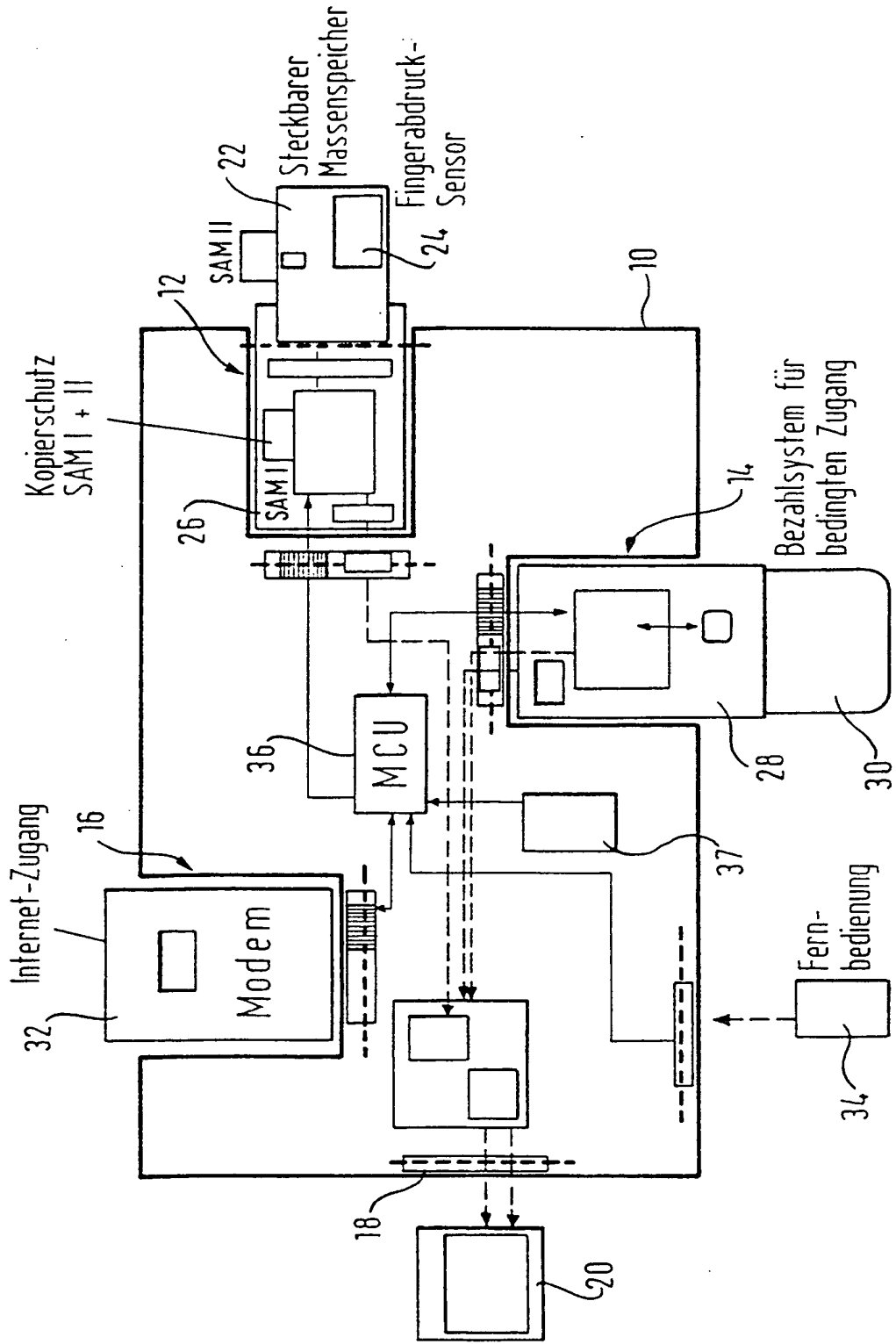
10 19. Wiedergabesystem nach Anspruch 16, ferner gekennzeichnet durch ein auf einem Chipkartenleser basierendes Bezahlungssystem für bedingten Zugang zu einem Datenanbieter über ein entferntes Netzwerk.

15 20. Wiedergabesystem nach Anspruch 17, dadurch gekennzeichnet, daß der Chipkartenleser als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

20 21. Wiedergabesystem nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß eine Überwachungseinrichtung vorgesehen ist, die einen mit den Daten vom Massenspeicher gelesenen zertifizierten Zeitstempel auswertet.

3 Page Blank (uspto)

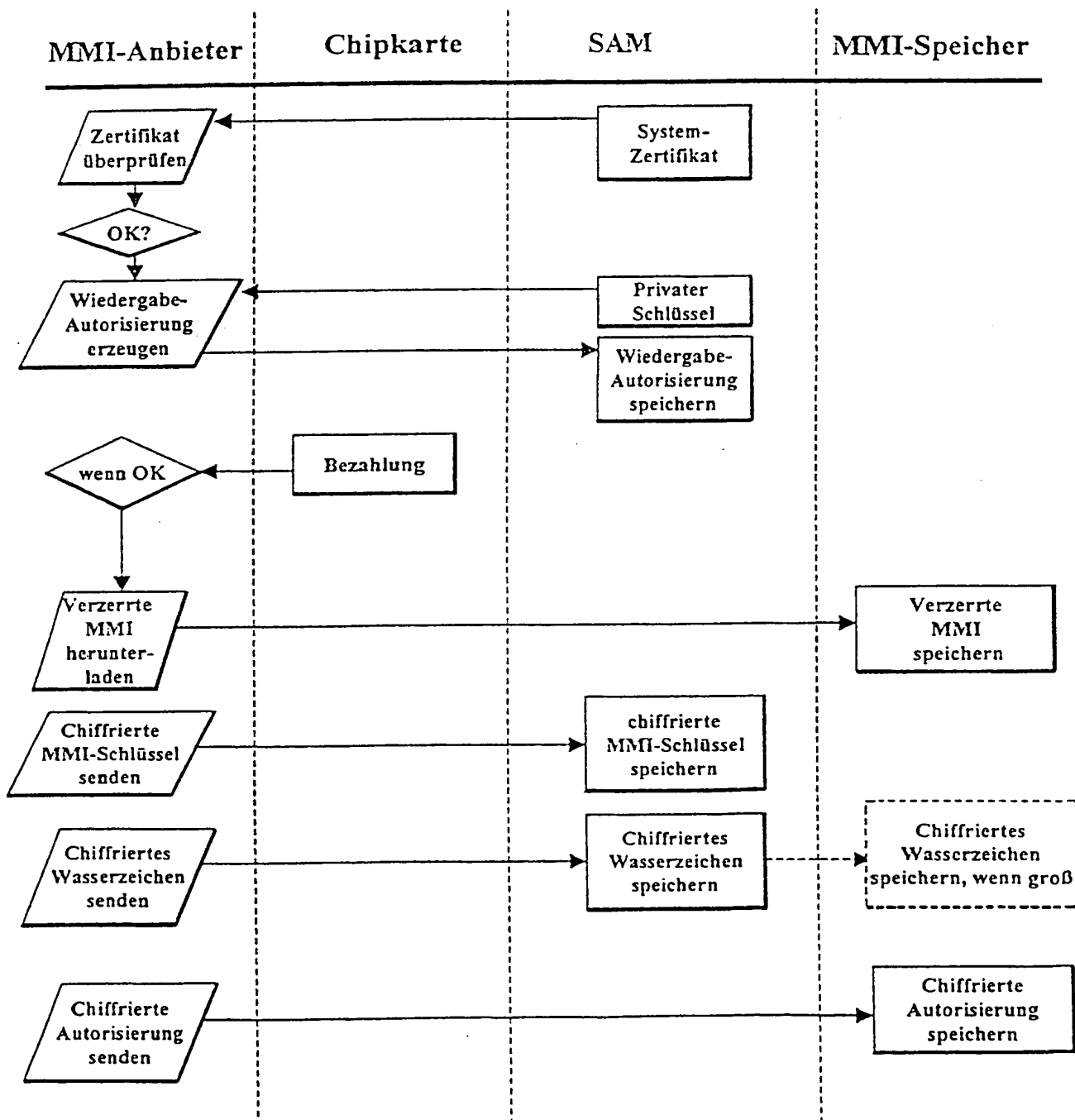
Fig. 1



This Page Blank (uspto)

Fig. 2

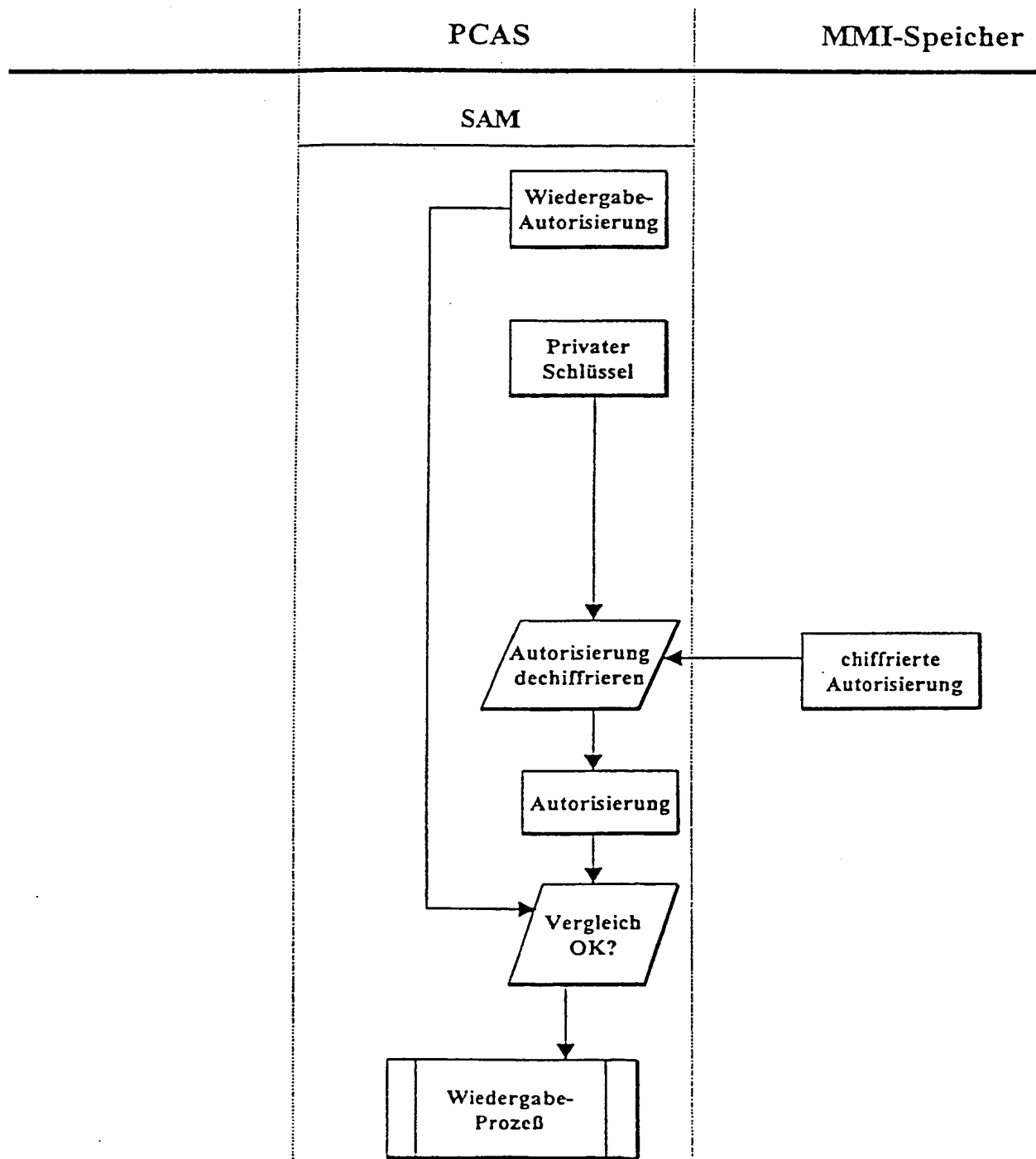
Personalisierung MMI-Massenspeicher



This Page Blank (uspto)

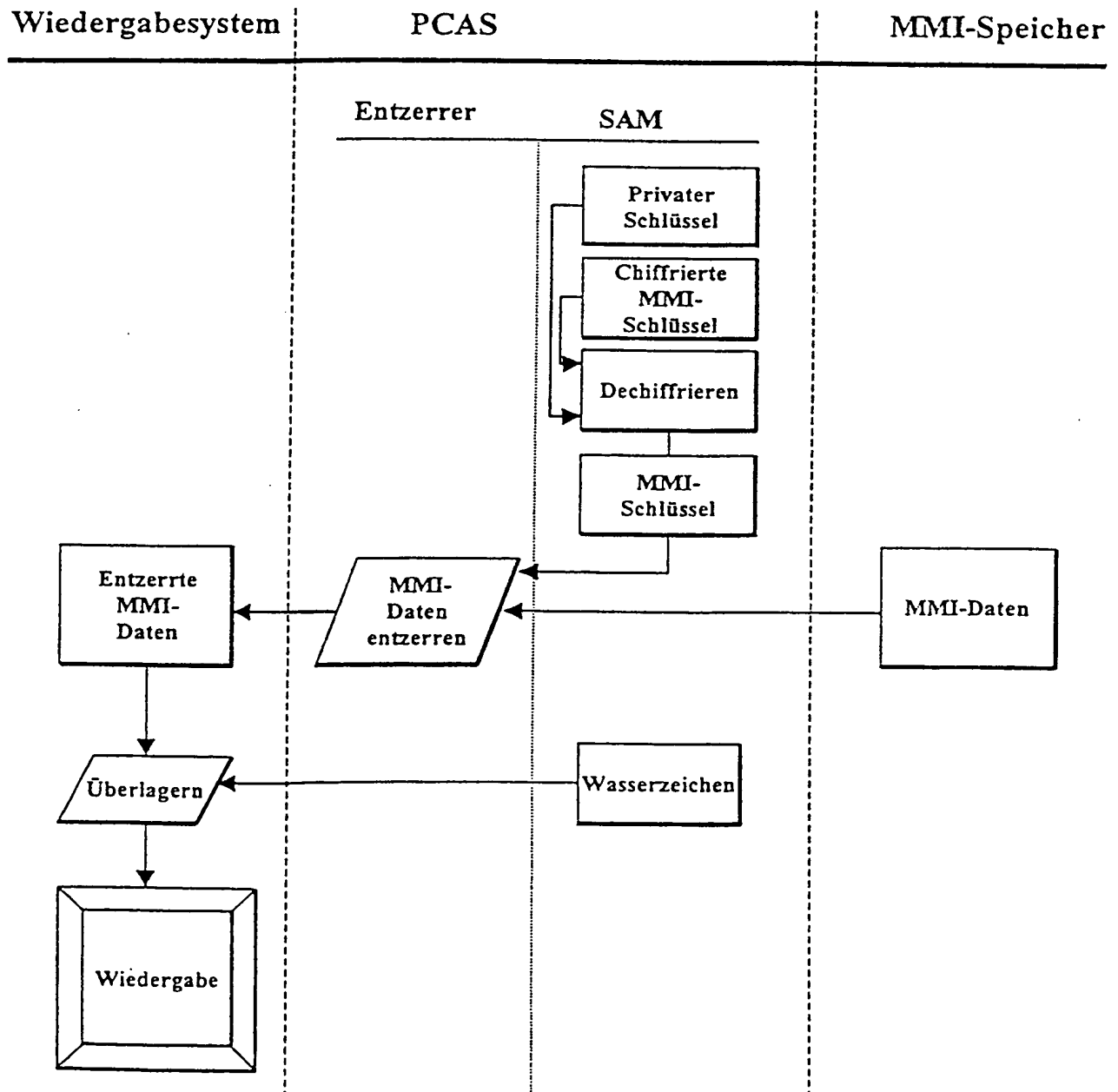
Fig. 3

Überprüfung Wiedergabe-Autorisierung



This Page Blank (uspto)

Fig. 4
Wiedergabe-Prozeß



This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/02414

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F G11B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 298 02 270 U (SCM MICROSYSTEMS GMBH) 30 April 1998 (1998-04-30) page 1 -page 17 figures 1-5 ---	1,2, 5-15, 18-20
A	DE 298 05 046 U (SCM MICROSYSTEMS GMBH) 23 July 1998 (1998-07-23) page 1 -page 5 figures 1,2 ---	1,2,6, 8-15, 18-20
A	EP 0 191 162 A (IBM) 20 August 1986 (1986-08-20) abstract column 6, line 8 -column 11, line 16 --- -/--	1-3,6, 10-18, 20,21

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

14 August 2000

Date of mailing of the international search report

22/08/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Jacobs, P

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 00/02414

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 302 710 A (IBM) 8 February 1989 (1989-02-08) abstract page 2 -page 5 ---	1,3,6, 8-12,16, 18
A	WO 96 35987 A (MACROVISION CORP) 14 November 1996 (1996-11-14) page 9 -page 14, line 2 ---	1,6, 8-13,18, 20
A	EP 0 844 550 A (AT & T CORP) 27 May 1998 (1998-05-27) -----	

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/EP 00/02414

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 29802270	U	30-04-1998	WO	9941909 A	19-08-1999
DE 29805046	U	23-07-1998	WO	9948284 A	23-09-1999
EP 0191162	A	20-08-1986	CA	1238427 A	21-06-1988
			DE	3587072 A	18-03-1993
			DE	3587072 T	12-08-1993
			JP	1630801 C	26-12-1991
			JP	2060007 B	14-12-1990
			JP	61145642 A	03-07-1986
			US	4757534 A	12-07-1988
EP 0302710	A	08-02-1989	US	4866769 A	12-09-1989
			CA	1292791 A	03-12-1991
			JP	1044542 A	16-02-1989
WO 9635987	A	14-11-1996	AU	702649 B	25-02-1999
			AU	6029896 A	29-11-1996
			BG	101999 A	31-07-1998
			BR	9609249 A	18-05-1999
			CA	2218383 A	14-11-1996
			CN	1185217 A	17-06-1998
			EP	0879533 A	25-11-1998
			JP	11505658 T	21-05-1999
			NZ	309989 A	29-03-1999
			PL	325440 A	20-07-1998
			US	5754648 A	19-05-1998
			US	5754649 A	19-05-1998
EP 0844550	A	27-05-1998	US	6005935 A	21-12-1999
			JP	10240520 A	11-09-1998

This Page Blank (uspto)

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G06F1/00 G11B20/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06F G11B G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 298 02 270 U (SCM MICROSYSTEMS GMBH) 30. April 1998 (1998-04-30) Seite 1 -Seite 17 Abbildungen 1-5 ---	1,2, 5-15, 18-20
A	DE 298 05 046 U (SCM MICROSYSTEMS GMBH) 23. Juli 1998 (1998-07-23) Seite 1 -Seite 5 Abbildungen 1,2 ---	1,2,6, 8-15, 18-20
A	EP 0 191 162 A (IBM) 20. August 1986 (1986-08-20) Zusammenfassung Spalte 6, Zeile 8 -Spalte 11, Zeile 16 --- -/-	1-3,6, 10-18, 20,21



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

14. August 2000

Absenddatum des internationalen Recherchenberichts

22/08/2000

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Jacobs, P

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 302 710 A (IBM) 8. Februar 1989 (1989-02-08) Zusammenfassung Seite 2 -Seite 5 ----	1,3,6, 8-12,16, 18
A	WO 96 35987 A (MACROVISION CORP) 14. November 1996 (1996-11-14) Seite 9 -Seite 14, Zeile 2 ----	1,6, 8-13,18, 20
A	EP 0 844 550 A (AT & T CORP) 27. Mai 1998 (1998-05-27) -----	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/02414

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 29802270 U	30-04-1998	WO 9941909 A	19-08-1999
DE 29805046 U	23-07-1998	WO 9948284 A	23-09-1999
EP 0191162 A	20-08-1986	CA 1238427 A	21-06-1988
		DE 3587072 A	18-03-1993
		DE 3587072 T	12-08-1993
		JP 1630801 C	26-12-1991
		JP 2060007 B	14-12-1990
		JP 61145642 A	03-07-1986
		US 4757534 A	12-07-1988
EP 0302710 A	08-02-1989	US 4866769 A	12-09-1989
		CA 1292791 A	03-12-1991
		JP 1044542 A	16-02-1989
WO 9635987 A	14-11-1996	AU 702649 B	25-02-1999
		AU 6029896 A	29-11-1996
		BG 101999 A	31-07-1998
		BR 9609249 A	18-05-1999
		CA 2218383 A	14-11-1996
		CN 1185217 A	17-06-1998
		EP 0879533 A	25-11-1998
		JP 11505658 T	21-05-1999
		NZ 309989 A	29-03-1999
		PL 325440 A	20-07-1998
		US 5754648 A	19-05-1998
		US 5754649 A	19-05-1998
EP 0844550 A	27-05-1998	US 6005935 A	21-12-1999
		JP 10240520 A	11-09-1998

This Page Blank (uspto)